



Milwaukee Police Department
Police Administration Building
749 West State Street
Milwaukee, Wisconsin 53233
<http://www.milwaukee.gov/police>

Alfonso Morales
Chief of Police

(414) 933-4444

September 6, 2019

MuckRock News
DEPT MR 75678
411A Highland Ave
Somerville, MA 02144-2516

Dear Emma Best:

This letter is in response to your records request dated June 21, 2019, in which you have made a request for records pursuant to the Wisconsin Public Records Law. Wis. Stat. §§ 19.31-39. You have requested:

- See attached request regarding "records mentioning, describing or generated as a result of the 8 May 2015 roll call release IA-0181-15 from the Department of Homeland Security's Office of Intelligence & Analysis."


The public policy in this state is to give the public the greatest amount of access to government records as possible. Wis. Stat. § 19.31. The general presumption is that government records are open to the public unless there is a clear statutory or common law exception. If there is no clear statutory or common law exception the custodian must "decide whether the strong presumption favoring access and disclosure is overcome by some even stronger public policy favoring limited access or nondisclosure." *Hempel v. City of Baraboo*, 2005 WI 120, § 28 (Citations omitted). Notwithstanding the presumption of openness, the public's right to access to public records is not absolute. *Journal/Sentinel v. Aagerup*, 145 Wis. 2d 818, 822 (Ct. App. 1988).

Upon review of your request and upon inspection of MPD's records, the records custodian has determined that there are no records that are responsive to your request regarding records mentioning, describing or generated as a result of the 8 May 2015 roll call release IA-0181-15 from the Department of Homeland Security's Office of Intelligence & Analysis. Under Wisconsin law, a records custodian need not create a new record in response to a records request for a nonexistent record. Wis. Stat. § 19.35(1)(L).

This determination is subject to review by *mandamus* action under Wis. Stat. § 19.37(1), or upon an application to the Wisconsin Attorney General or the Milwaukee County Corporation Counsel.

Sincerely,

ALFONSO MORALES
CHIEF OF POLICE


KERRY NAMIN
POLICE SERGEANT

AM:KN:sw
J11610 Reference Number

Wisconsin Open Records Act Request: Criminal Hackers Target Police to Protest Perceived Injustices (Milwaukee Police Department)

75678-13573194@requests.muckrock.com

Fri 6/21/2019 12:12 PM

To: Records, Open <mpdopenrecords@milwaukee.gov>;

1 attachments (259 KB)

DHS-FBI-HackersTargetPolice.pdf;

Milwaukee Police Department
ORA Office
P.O. Box 531
Milwaukee, WI 53210

June 21, 2019

To Whom It May Concern:

Pursuant to the Wisconsin Open Records Act, I hereby request the following records:

Records mentioning, describing or generated as a result of the 8 May 2015 Roll Call Release IA-0181-15 (which was designed to be shared widely with law enforcement) from the Department of Homeland Security's Office of Intelligence and Analysis (I&A) in conjunction with the Federal Bureau of Investigation, titled "Criminal Hackers Target Police to Protest Perceived Injustices," as well as records otherwise responding or reacting to the issues raised in it.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 business days.

JUL 10

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 75678-13573194@requests.muckrock.com

Upload documents directly: https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAVzfaRyXCKHY6hk-qPhCrBLjc%3A1heN5l%3AFE-Zdbf-3AqHs4d2palhQMw3HCY&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fmilwaukee-police-department-653%252Fcriminal-hackers-target-police-to-protest-perceived-injustices-milwaukee-police-department-75678%252F%253Femail%253Dmpdopenrecords%252540milwaukee.gov

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 75678

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



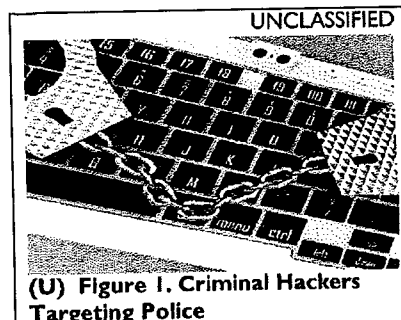
ROLL CALL RELEASE

INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.



(U) Figure 1. Criminal Hackers Targeting Police

- » (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.
- » (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.
- » (U//FOUO) A criminal hacker using the moniker (at)DigaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.

(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

- » (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
- » (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
- » (U) Conduct rate-limiting of traffic at the network perimeter, and
- » (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

- » (U) Execute ISP address rotation,
- » (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
- » (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information:

http://msisac.cisecurity.org/resources/reports/documents/GuidetoDDoSAttacks_000.pdf.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0181-15

(U) Prepared by the Office of Intelligence and Analysis (IA). Coordinated with the FBI. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.